

BEST AVAILABLE COPY
PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-117587
(43)Date of publication of application : 28.04.2005

(51)Int.Cl. H04L 12/46

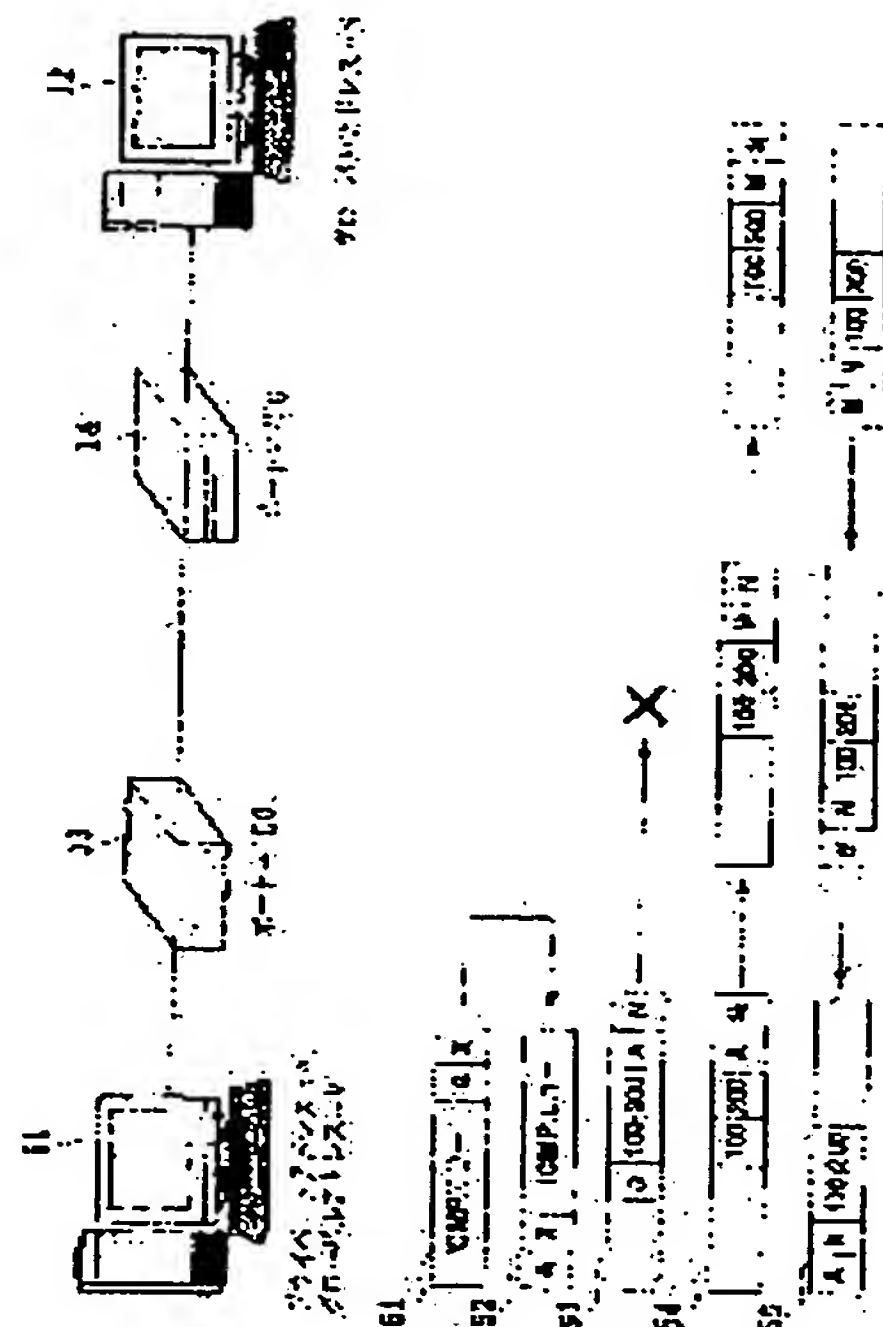
(21)Application number : 2003-352950 (71)Applicant : NEWRONG INC
(22)Date of filing : 10.10.2003 (72)Inventor : YAMADA IKUYA
SATO DAISUKE
SUNOCHI YUJI
ARAKI EIJI
KONOSE TOMOYUKI

(54) COMMUNICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To certainly realize P2P application even in connection environment using NAT function.

SOLUTION: The method is provided with a 1st step for transmitting two or more echo packets 51 from a host computer 11 to a router 13 in which setting value of TTL increases one by one from one, a 2nd step for responding to one out of a plurality of echo packets, receiving an echo packet 52 returned from the router 13, and extracting the setting value of the TTL for the returned echo packet 51, and a 3rd step for transmitting a port setting packet 53 making the TTL setting value to be a by adding 1 to the extracted setting value from the host computer 11 to the router 13.



LEGAL STATUS

[Date of request for examination] 18.01.2005
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号
特開2005-117587
(P2005-117587A)

(43) 公開日 平成17年4月28日(2005.4.28)

(51) Int. Cl.⁷
H04L 12/46

F I
H04L 12/46

E

テーマコード (参考)
5K033

審査請求 有 請求項の数 8 O L (全 11 頁)

| | | | |
|-----------|------------------------------|----------|---|
| (21) 出願番号 | 特願2003-352950 (P2003-352950) | (71) 出願人 | 503373034 株式会社ニューロン 神奈川県藤沢市湘南台1-7-4 |
| (22) 出願日 | 平成15年10月10日 (2003.10.10) | (74) 代理人 | 100077481 弁理士 谷 義一 |
| | | (74) 代理人 | 100088915 弁理士 阿部 和夫 |
| | | (72) 発明者 | 山田 育矢 神奈川県藤沢市湘南台1-7-4 株式会 社ニューロン内 |
| | | (72) 発明者 | 佐藤 大介 神奈川県藤沢市湘南台1-7-4 株式会 社ニューロン内 |

最終頁に続く

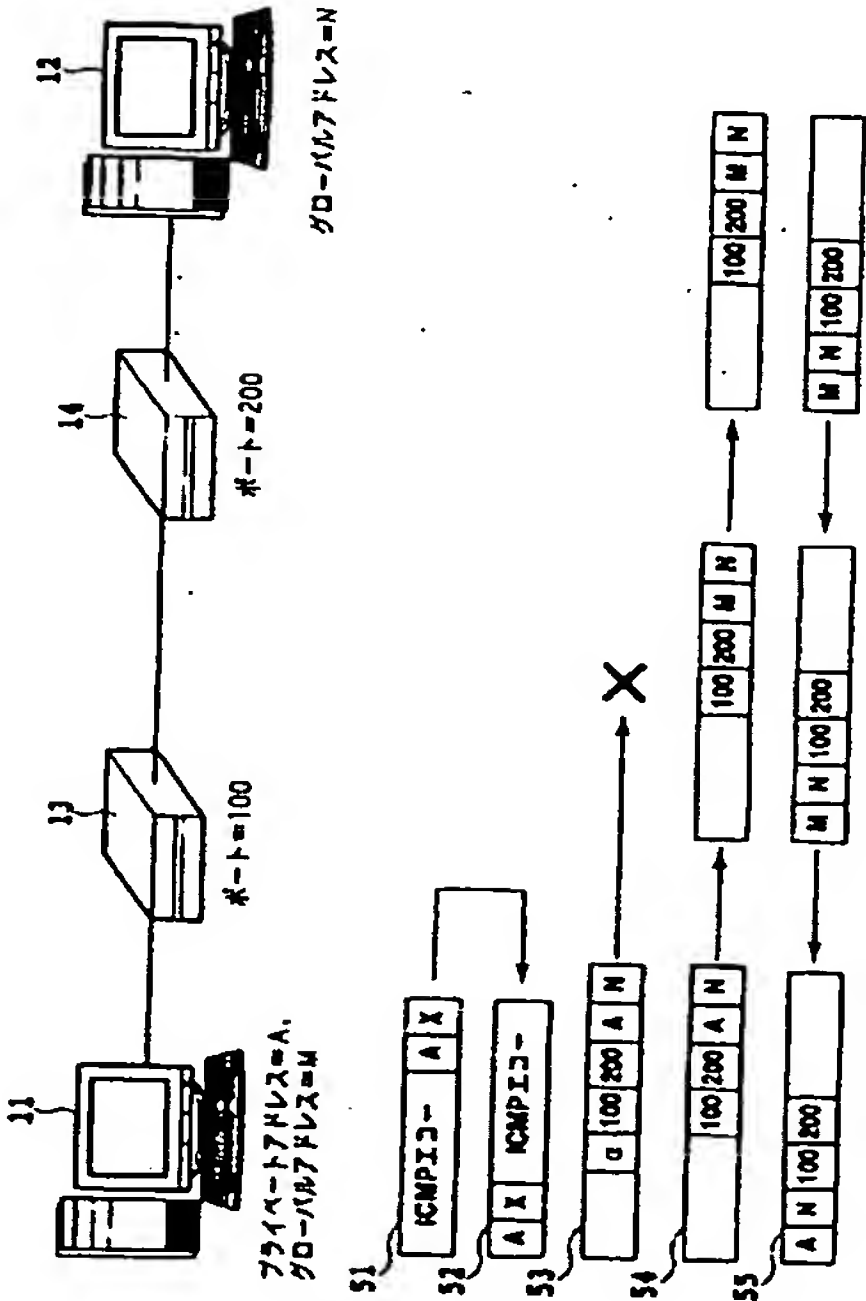
(54) 【発明の名称】 通信方法

(57) 【要約】

【課題】 NAT機能を利用した接続環境においても、確実にP2Pアプリケーションを実現する。

【解決手段】 ホストコンピュータ11からルータ13へ、TTLの設定値を1から1ずつ増やした複数のエコーパケット51を送信する第1ステップと、複数のエコーパケットのうちの1つに応答して、ルータ13から返送されたエコーパケット52を受信し、ホスト11が返送されたエコーパケット51のTTLの設定値を抽出する第2ステップと、ホスト11からルータ13へ、TTLの設定値を抽出された設定値に1を加えた値αとしたポート設定パケット53を送信する第3ステップとを備えた。

【選択図】 図3



【特許請求の範囲】

【請求項 1】

NAT機能を有するネットワーク機器に接続されたコンピュータからP2P型通信を行うための通信方法において、

前記コンピュータから前記ネットワーク機器へ、TTLの設定値を1から1ずつ増やした複数のエコーパケットを送信する第1ステップと、

前記複数のエコーパケットのうちの1つに回答して、前記ネットワーク機器から返送されたエコーパケットを受信し、前記コンピュータが前記返送されたエコーパケットのTTLの設定値を抽出する第2ステップと、

前記コンピュータから前記ネットワーク機器へ、TTLの設定値を前記抽出された設定値に1を加えた値としたポート設定パケットを送信する第3ステップと

を備えたことを特徴とする通信方法。

10

【請求項 2】

前記コンピュータから前記ネットワーク機器へ、TTLの設定値を前記抽出された設定値に1を加えた値としたキープアライブパケットを、通信が中断している間、一定時間間隔で送信する第4ステップをさらに備えたことを特徴とする請求項1に記載の通信方法。

【請求項 3】

NAT機能を有するネットワーク機器に接続されたコンピュータからP2P型通信を行うための通信方法において、

前記コンピュータから前記ネットワーク機器へエコーパケットを送信して、前記コンピュータから前記ネットワーク機器までのホップ数を取得する第1ステップと、

前記コンピュータから前記ネットワーク機器へ、前記取得されたホップ数に1を加えた値をTTLの設定値としたキープアライブパケットを、通信が中断している間、一定時間間隔で送信する第2ステップと

を備えたことを特徴とする通信方法。

20

【請求項 4】

前記パケットは、パケットの種別を示すフラグを有し、前記コンピュータおよび前記ネットワーク機器は、前記ポート設定パケットおよび前記キープアライブパケットとその他のパケットとを、前記フラグにより識別することを特徴とする請求項1、2または3に記載の通信方法。

30

【請求項 5】

NAT機能を有するネットワーク機器に接続されたコンピュータからP2P型通信を行うための通信方法において、

前記コンピュータから前記ネットワーク機器を介してセッション管理サーバへ、異なるソケットペアの複数のパケットを送信する第1ステップと、

前記セッション管理サーバが前記パケットから抽出した送信元ポート番号を含む応答パケットを、前記セッション管理サーバから受信し、前記コンピュータが前記応答パケットの前記送信元ポート番号を抽出する第2ステップと、

前記コンピュータが、抽出された複数の前記送信元ポート番号から、インクリメント数を算出する第3ステップと

を備えたことを特徴とする通信方法。

40

【請求項 6】

前記コンピュータから前記ネットワーク機器を介して前記セッション管理サーバへパケットを送信し、該パケットの応答パケットから、前記ネットワーク機器のポート番号を取得する第4ステップと、

前記コンピュータから前記セッション管理サーバへ、前記第4ステップで取得した前記ポート番号に前記インクリメント数を加えた値を送信元ポート番号に設定したパケットを送信し、該パケットの応答パケットから、前記P2P型通信の相手先のネットワーク機器のポート番号を取得する第5ステップと、

前記インクリメント数を加えた値を送信元ポート番号として設定し、前記第5ステップ

50

で取得した前記ポート番号を宛先ポート番号として設定したパケットを送信する第6ステップと

をさらに備えたことを特徴とする請求項5に記載の通信方法。

【請求項7】

P2P型通信を行うために、NAT機能を有するネットワーク機器に接続されたコンピュータに、請求項1ないし6のいずれかに記載の各ステップを実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項8】

P2P型通信を行うために、NAT機能を有するネットワーク機器に接続されたコンピュータに、請求項1ないし6のいずれかに記載の各ステップを実行させるためのプログラム

10

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、通信方法に関し、より詳細には、NAT機能を有するネットワーク機器に接続されたコンピュータからP2P型通信を行うための通信方法に関する。

【背景技術】

【0002】

近年、インターネットに接続するホストコンピュータの増大により、IPアドレスの不足という問題が顕著化している。そこで、IPアドレスの不足を解消するための一つの方法として、NAT (Network Address Translator) 機能が利用されている。NAT機能は、閉域網であるLAN内のプライベートアドレスを有するホストコンピュータと、インターネット内のグローバルアドレスを有するホストコンピュータとの間で通信を行うために、アドレス変換を行う。

20

【0003】

図1に、NAT機能を説明するためのネットワーク接続図を示す。ホスト11には、プライベートアドレスAとグローバルアドレスMとが割り当てられている。ルータ13には、NAT機能が実装されており、プライベートアドレスをグローバルアドレスに変換するための変換テーブルが格納されている。ここでホスト11からインターネット内のホスト12 (グローバルアドレスN) へ、ルータ13、14を介してIPパケットを送信する。ホスト11から送信されるIPパケットのヘッダには、宛先アドレス21として「N」、送信元アドレス22として「A」が書き込まれ、TCPヘッダまたはUDPヘッダには、宛先ポート番号23として「200」、送信元ポート番号24として「100」が書き込まれている。ルータ13は、変換テーブルを参照して、送信元アドレス22のプライベートアドレスAをグローバルアドレスMに変換し、ルータ14に向けてパケットを送信する。

30

【0004】

次に、ホスト12からホスト11へ、ルータ14、13を介してIPパケットを送信する。ホスト12から送信されるIPパケットのヘッダには、宛先アドレス31として「M」、送信元アドレス32として「N」が書き込まれ、TCPヘッダまたはUDPヘッダには、宛先ポート番号33として「100」、送信元ポート番号34として「200」が書き込まれている。ルータ13は、変換テーブルを参照して、宛先アドレス31のグローバルアドレスMをプライベートアドレスAに変換し、LAN内のホスト11に向けてパケットを送信する。

40

【0005】

一方、オンラインゲームやビデオチャットなどのP2P (peer to peer) 型通信を利用したアプリケーション (以下、P2Pアプリケーションという) の利用が増えている。P2P型通信は、サーバを介さずに、端末間で直接通信をおこなう。NAT機能を利用した接続環境において、P2Pアプリケーションを利用するために、IETF (Internet Engineering Task Force) の規格であるSTUN (例えば、非特許文献1参照) 技術が知ら

50

れている。

【 0 0 0 6 】

【非特許文献1】REC3489 “STUN-Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)” March 2003

【発明の開示】

【発明が解決しようとする課題】

【 0 0 0 7 】

しかしながら、STUN技術によっても端末間で通信ができない場合があるという問題があった。規格が詳細な部分まで規定されていなかったり、ルータによって実装する部分が異なるためである。具体的な例を以下に説明する。

10

【 0 0 0 8 】

図2に、ICMPパケットによりブロックを行う場合を示す。ホスト11が、ホスト12に向け、ルータ14のポート番号「200」を宛先ポート番号としてパケット41を送信する。このとき、ルータ14が、ポート番号「200」を使用していない場合には、ICMPパケット（宛先到達不能メッセージ）42をルータ13に返送する。ルータ13は、ICMPパケット42を受信すると、送信元ポート番号「100」のポートを閉じるようになっている。従って、以後ホスト11が、ホスト12に向けてパケット43を送信しても、ルータ13はパケット43を受け付けない。

【 0 0 0 9 】

また、ルータ内に格納されている変換テーブルの内容は、通信が中断してから一定時間が経過すると、削除されてしまう。すなわち、宛先アドレス、送信元アドレス、宛先ポート番号、および送信元ポート番号の関係がクリアされてしまい、ルータ13は、同一のアドレス、同一のポート番号を設定したパケットを受け付けない。

20

【 0 0 1 0 】

さらに、シンメトリックルータと呼ばれるルータは、宛先ポート番号、宛先アドレスが変わるごとに、自身のポート番号、すなわち送信元ポート番号を変えてしまう。従って、同一のセッションで異なる宛先ポート番号にパケットを送信すると、以後同一の送信元ポート番号を使用してパケットを送信することができない。

【 0 0 1 1 】

本発明は、このような問題に鑑みてなされたもので、その目的とするところは、NAT機能を利用した接続環境においても、確実にP2Pアプリケーションを実現するための通信方法を提供することにある。

30

【課題を解決するための手段】

【 0 0 1 2 】

本発明は、このような目的を達成するために、請求項1に記載の発明は、NAT機能を有するネットワーク機器に接続されたコンピュータからP2P型通信を行うための通信方法において、前記コンピュータから前記ネットワーク機器へ、TTLの設定値を1から1ずつ増やした複数のエコーパケットを送信する第1ステップと、前記複数のエコーパケットのうちの1つに応答して、前記ネットワーク機器から返送されたエコーパケットを受信し、前記コンピュータが前記返送されたエコーパケットのTTLの設定値を抽出する第2ステップと、前記コンピュータから前記ネットワーク機器へ、TTLの設定値を前記抽出された設定値に1を加えた値としたポート設定パケットを送信する第3ステップとを備えたことを特徴とする。

40

【 0 0 1 3 】

請求項2に記載の発明は、請求項1に記載の通信方法において、前記コンピュータから前記ネットワーク機器へ、TTLの設定値を前記抽出された設定値に1を加えた値としたキープアライブパケットを、通信が中断している間、一定時間間隔で送信する第4ステップをさらに備えたことを特徴とする。

【 0 0 1 4 】

請求項3に記載の発明は、NAT機能を有するネットワーク機器に接続されたコンピュ

50

ータからP2P型通信を行うための通信方法において、前記コンピュータから前記ネットワーク機器へエコーパケットを送信して、前記コンピュータから前記ネットワーク機器までのホップ数を取得する第1ステップと、前記コンピュータから前記ネットワーク機器へ、前記取得されたホップ数に1を加えた値をTTLの設定値としたキープアライブパケットを、通信が中断している間、一定時間間隔で送信する第2ステップとを備えたことを特徴とする。

【0015】

請求項4に記載の発明は、請求項1、2または3に記載の前記パケットは、パケットの種別を示すフラグを有し、前記コンピュータおよび前記ネットワーク機器は、前記ポート設定パケットおよび前記キープアライブパケットとその他のパケットとを、前記フラグにより識別することを特徴とする。

10

【0016】

請求項5に記載の発明は、NAT機能を有するネットワーク機器に接続されたコンピュータからP2P型通信を行うための通信方法において、前記コンピュータから前記ネットワーク機器を介してセッション管理サーバへ、異なるソケットペアの複数のパケットを送信する第1ステップと、前記セッション管理サーバが前記パケットから抽出した送信元ポート番号を含む応答パケットを、前記セッション管理サーバから受信し、前記コンピュータが前記応答パケットの前記送信元ポート番号を抽出する第2ステップと、前記コンピュータが、抽出された複数の前記送信元ポート番号から、インクリメント数を算出する第3ステップとを備えたことを特徴とする。

20

【0017】

請求項6に記載の発明は、請求項5に記載の通信方法において、前記コンピュータから前記ネットワーク機器を介して前記セッション管理サーバへパケットを送信し、該パケットの応答パケットから、前記ネットワーク機器のポート番号を取得する第4ステップと、前記コンピュータから前記セッション管理サーバへ、前記第4ステップで取得した前記ポート番号に前記インクリメント数を加えた値を送信元ポート番号に設定したパケットを送信し、該パケットの応答パケットから、前記P2P型通信の相手先のネットワーク機器のポート番号を取得する第5ステップと、前記インクリメント数を加えた値を送信元ポート番号として設定し、前記第5ステップで取得した前記ポート番号を宛先ポート番号として設定したパケットを送信する第6ステップとをさらに備えたことを特徴とする。

30

【0018】

請求項7に記載の発明は、P2P型通信を行うために、NAT機能を有するネットワーク機器に接続されたコンピュータに、請求項1ないし6のいずれかに記載の各ステップを実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であることを特徴とする。

【0019】

請求項8に記載の発明は、P2P型通信を行うために、NAT機能を有するネットワーク機器に接続されたコンピュータに、請求項1ないし6のいずれかに記載の各ステップを実行させるためのプログラムであることを特徴とする。

【発明の効果】

40

【0020】

以上説明したように、本発明によれば、通信の開始から終了まで、ネットワーク機器における所定のポートを常にかいておくことができるので、NAT機能を利用した接続環境においても、確実にP2Pアプリケーションを実現することが可能となる。

【発明を実施するための最良の形態】

【0021】

以下、図面を参照しながら本発明の実施形態について詳細に説明する。上述したように、NAT機能を利用した接続環境において、P2Pアプリケーションを実現するためには、通信の開始から終了まで、ルータにおける所定のポートを常にかいておく必要がある。そこで、通信の最初にポートを開いておく方法、いったん開いたポートを維持する方法、

50

通信中のポート番号の変更に対応する方法を順次説明する。

【0022】

図3に、本発明の第1の実施形態にかかるP2P通信方法を示す。端末間でP2P通信を行う場合には、ICMP packetsによるブロックを避けて、最初に、セッションで使用するルータのポートを開いておく必要がある。そこで、ルータ13までのホップ数を調べ、ポートを開けるためのUDP packetsを送信する。

【0023】

具体的には、ホスト11でICMPのエコー packets を生成し、TTL (Time To Live) = 1で送信する。順次、TTL = 2, 3...と増やして、複数のエコー packets を送信する。TTLの数値がルータ13のホップ数と等しいエコー packets 51を送信すると、ルータ13よりエコー packets 52がホスト11に返送される。ホスト11は、返送されたエコー packets 52により、ルータ13までのホップ数を知ることができる。

10

【0024】

次に、ホスト11は、ルータ13のホップ数に1を加えた値 α をTTLに設定し、送信元ポート番号「100」のポート設定 packets 53を送信する。これによって、ルータ13の送信元ポート番号「100」のポートが開かれる。ポート設定 packets 53は、ルータ13の次のホップで削除されるので、他の通信に影響を与えることはない。

【0025】

このような構成により、ルータ13の送信元ポート番号「100」のポートを開けておくことにより、packets 54, 55による端末間の通信を行うことができる。このとき、ルータ14もICMP packetsによりブロックを行う機能を有している場合には、ホスト12においても、同様の処理を行う。

20

【0026】

図4に、本発明の第2の実施形態にかかるP2P通信方法を示す。同一のセッションにおいて、packetsの送受信が途絶えている間は、ルータが変換テーブルをクリアしないように、いったん開いたポートを維持しておく必要がある。そこで、packetsの送受信が途絶えている間は、キープアライブ packets を一定時間間隔で送信する。例えば、上述したICMPエコー packets を利用して、ルータ13までのホップ数を予め調べておく。ホスト11は、ルータ13のホップ数に1を加えた値 α をTTLに設定し、送信元ポート番号「100」のUDP packets 61を送信する。これによって、ルータ13に格納されている変換テーブルの内容は削除されず、以後、同一のポート番号を設定した packets を送信することができる。

30

【0027】

なお、第1および第2の実施形態においては、ICMP packetsによりブロックを行う機能を有しているルータにのみ送信するようにしてもよい。ルータによっては、TTLの設定値が α の場合に、packetsを破棄してポートを閉じてしまう機能を有する場合があるからである。

【0028】

ポート設定 packets およびキープアライブ packets が他のホストに到達した場合に、通信の混乱が起こらないようにする。例えば、図4に示したように、全ての packets の先頭に、フラグ63, 64を付加し、キープアライブ packets の場合は「1」を、通常の packets の場合は「0」を設定する。このようにして、ホストがキープアライブ packets を受信した場合でも、これを識別して破棄することができる。

40

【0029】

図5に、本発明の第3の実施形態にかかるP2P通信方法を示す。シンメトリックルータなど通信中のポート番号の変更に対応する方法を説明する。ルータ13は、シンメトリックルータであり、宛先ポート番号、宛先アドレスが変わるごとに、自身のポート番号を2ずつインクリメントする。ルータ14も、シンメトリックルータであり、自身のポート番号を5ずつインクリメントする。このような場合に、ホスト11, 12は、セッション管理サーバ15を介して、ポート番号を予測しながら通信を行う。

50

【0030】

図6に、本発明の一実施形態にかかるポート番号の予測方法を示す。ホスト11, 12における予測方法の処理の流れを示している。最初に、ホスト11, 12は、セッション管理サーバ15からポートチェック1パケットを受信する(S102)。ポートチェック1パケットは、ホスト11, 12において、ルータ13, 14のポート番号のインクリメント数を調べさせるための指示パケットである。ポートチェック1パケットを受信したホスト11, 12は、新しいソケットペア、すなわち宛先ポート番号、宛先アドレスの少なくともいずれかを変えたUDPパケットを、セッション管理サーバ15に送信する(S104)。

【0031】

セッション管理サーバ15は、受信したUDPパケットから送信元ポート番号、すなわち変更されたルータ13, 14のポート番号を抽出して、ホスト11, 12に回答パケットを送信する(S106)。ホスト11, 12は、さらに、新しいソケットペアでn回繰り返してUDPパケットを、セッション管理サーバ15に送信する(S108)。

【0032】

ホスト11, 12は、UDPパケットをn回送信した後、受信した回答パケットから、ルータ13, 14のn個のポート番号を取得する。ホスト11, 12は、得られたポート番号からインクリメント数を算出する(S110)。算出の方法は、例えば、取得したポート番号の差分の平均値とする。差分の最大値と最小値を除いて、平均を算出するなどの計算方法を用いることもできる。

【0033】

図7に、予測されたポート番号に基づいたP2P通信方法を示す。最初に、ホスト11, 12は、セッション管理サーバ15にポートチェック2パケットを送信する(S202)。ポートチェック2パケットは、ルータ13, 14のポート番号を調べるための指示パケットである。ポートチェック2パケットを受信したセッション管理サーバ15は、受信したUDPパケットから送信元ポート番号を抽出して、ホスト11, 12に送信する(S204)。

【0034】

ホスト11, 12は、受信した送信元ポート番号に、図6に示した予測方法により取得したインクリメント数を加算して、セッション管理サーバ15にポートチェック3パケットを送信する(S206)。ポートチェック3パケットを受信したセッション管理サーバ15は、通信の相手先として各々対応するルータのポート番号を抽出して、ホスト11, 12に送信する(S208)。ホスト11, 12は、ステップS206で使用した送信元ポート番号と、ステップS208で受信したポート番号を宛先ポート番号として設定して、通常のパケットの送受信を行う。

【0035】

この構成によれば、通信を行うホスト11, 12は、セッション管理サーバ15を介して、常に正確なポート番号を予測することができるので、シンメトリックルータを介したP2Pアプリケーションを実現することができる。

【0036】

本実施形態によれば、通信の開始から終了まで、ルータにおける所定のポートを常に開いておくために、ICMPパケットによるブロックを避けて、通信の最初にポートを開いておくことができ、いったん開いたポートを維持して、通信中のポート番号の変更にも対応することができる。

【産業上の利用可能性】

【0037】

本発明は、NAT機能を利用した接続環境においても、確実にP2Pアプリケーションを実現することができるルータ、ゲートウェイなどのネットワーク機器に適用することができる。

【図面の簡単な説明】

10

20

30

40

50

【 0 0 3 8 】

【 図 1 】 N A T 機能を説明するためのネットワーク接続図である。

【 図 2 】 I C M P パケットによりブロックを行う機能を説明するためのネットワーク接続図である。

【 図 3 】 本発明の第 1 の実施形態にかかる P 2 P 通信方法を示すネットワーク接続図である。

【 図 4 】 本発明の第 2 の実施形態にかかる P 2 P 通信方法を示すネットワーク接続図である。

【 図 5 】 本発明の第 3 の実施形態にかかる P 2 P 通信方法を示すネットワーク接続図である。

【 図 6 】 本発明の一実施形態にかかるポート番号の予測方法を示すフローチャートである。

【 図 7 】 予測されたポート番号に基づいた P 2 P 通信方法を示すフローチャートである。

【 符号の説明 】

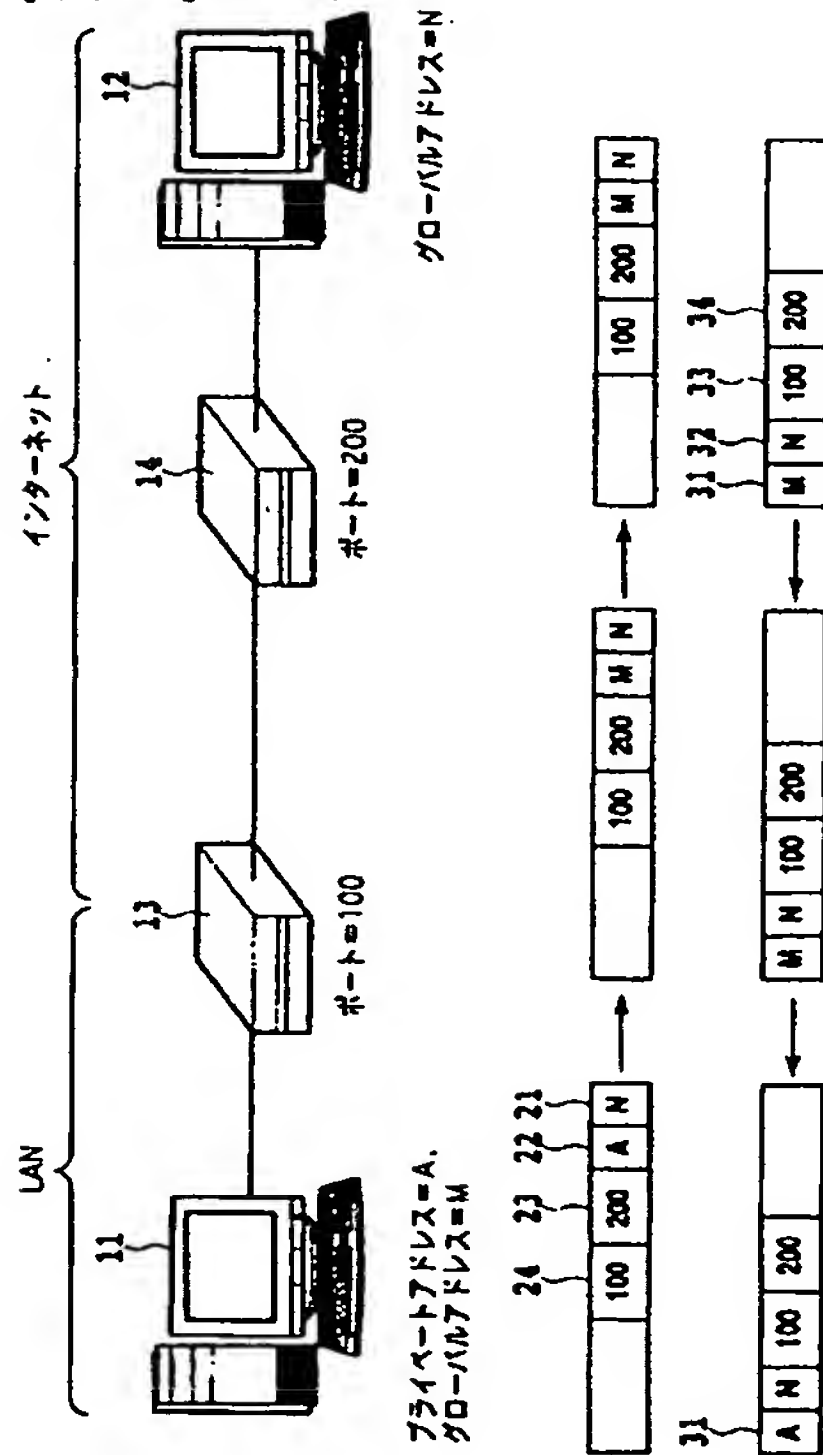
【 0 0 3 9 】

1 1, 1 2 ホスト

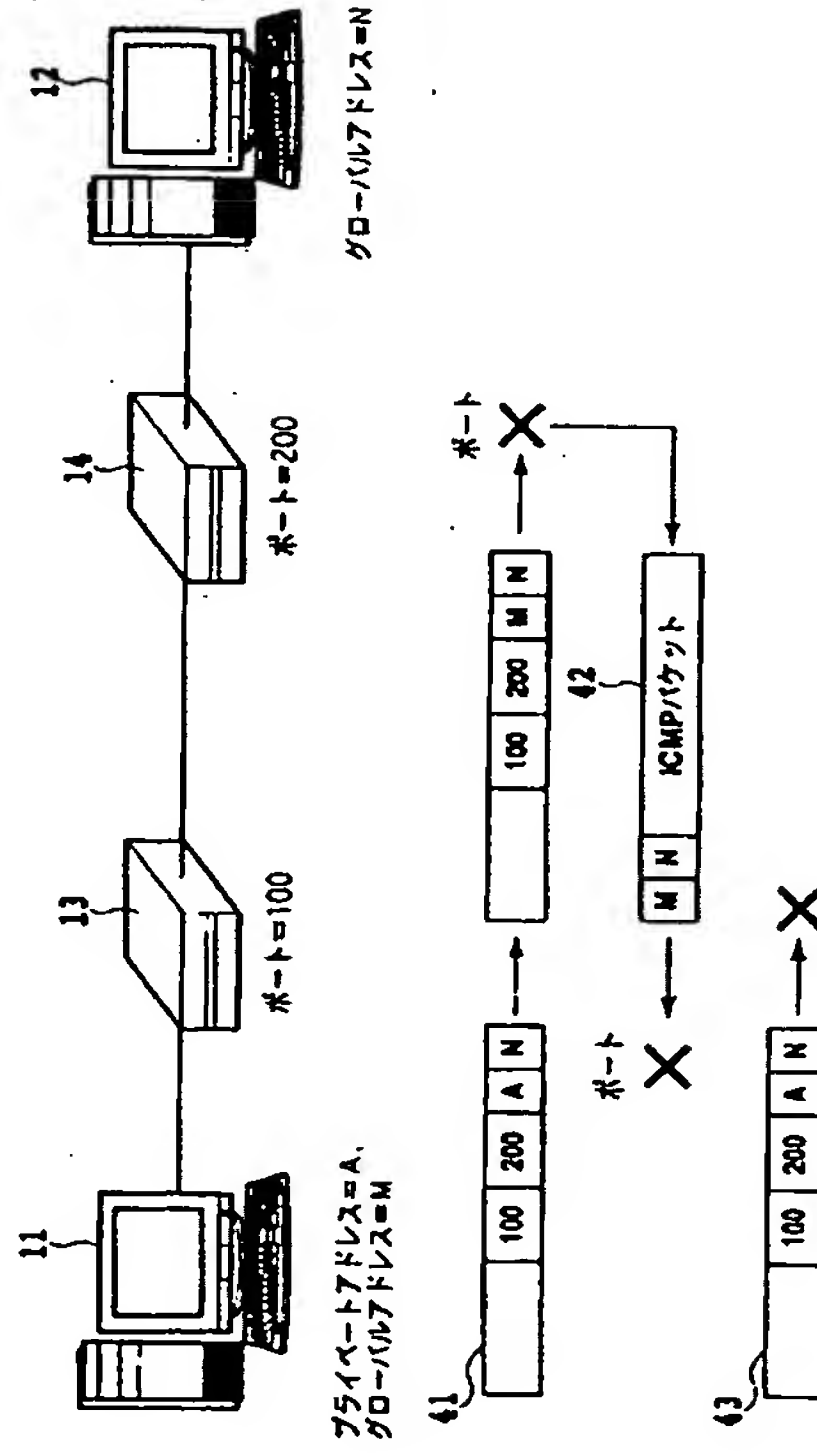
1 3, 1 4 ルータ

1 5 セッション管理サーバ

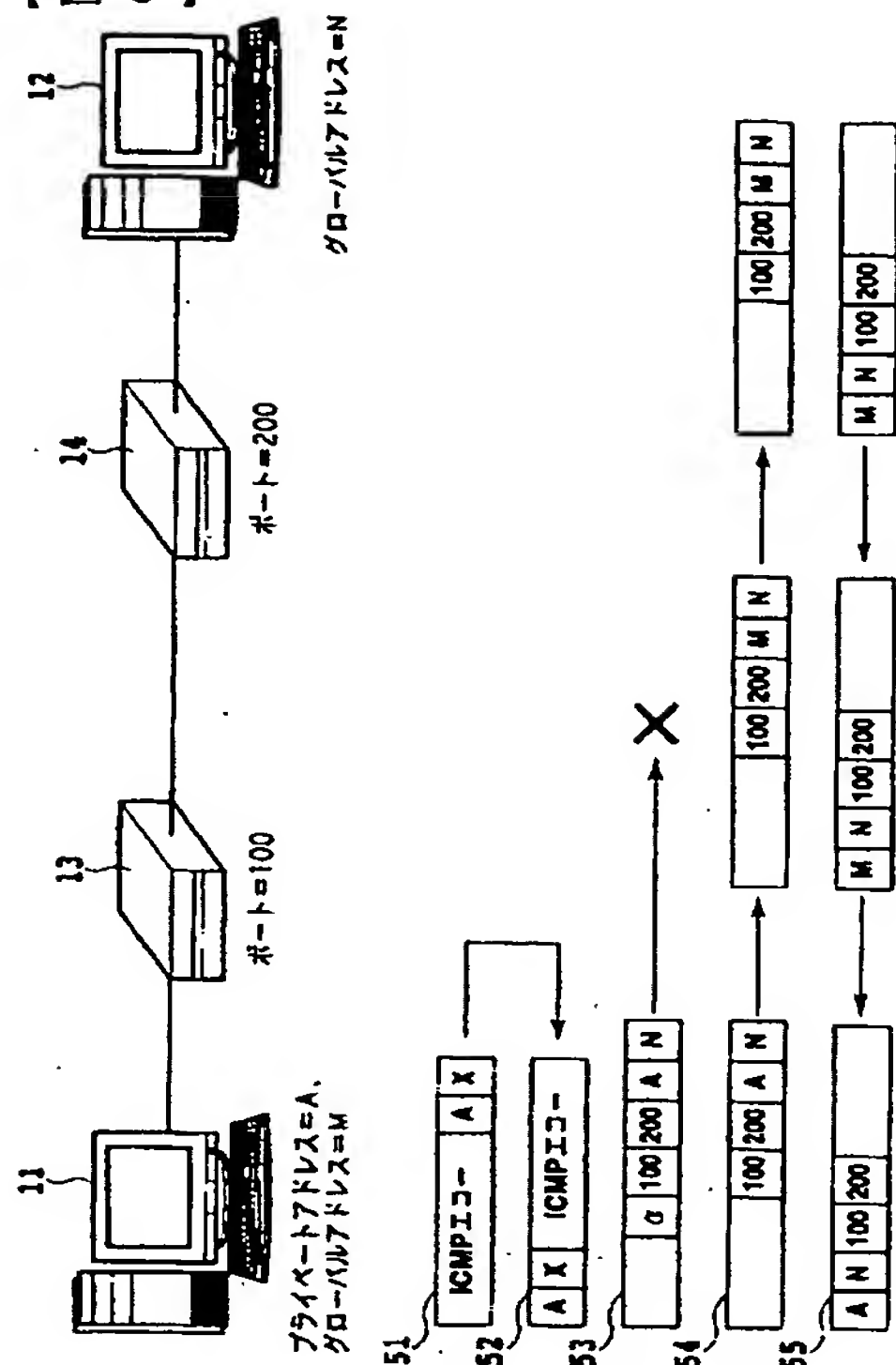
【 図 1 】



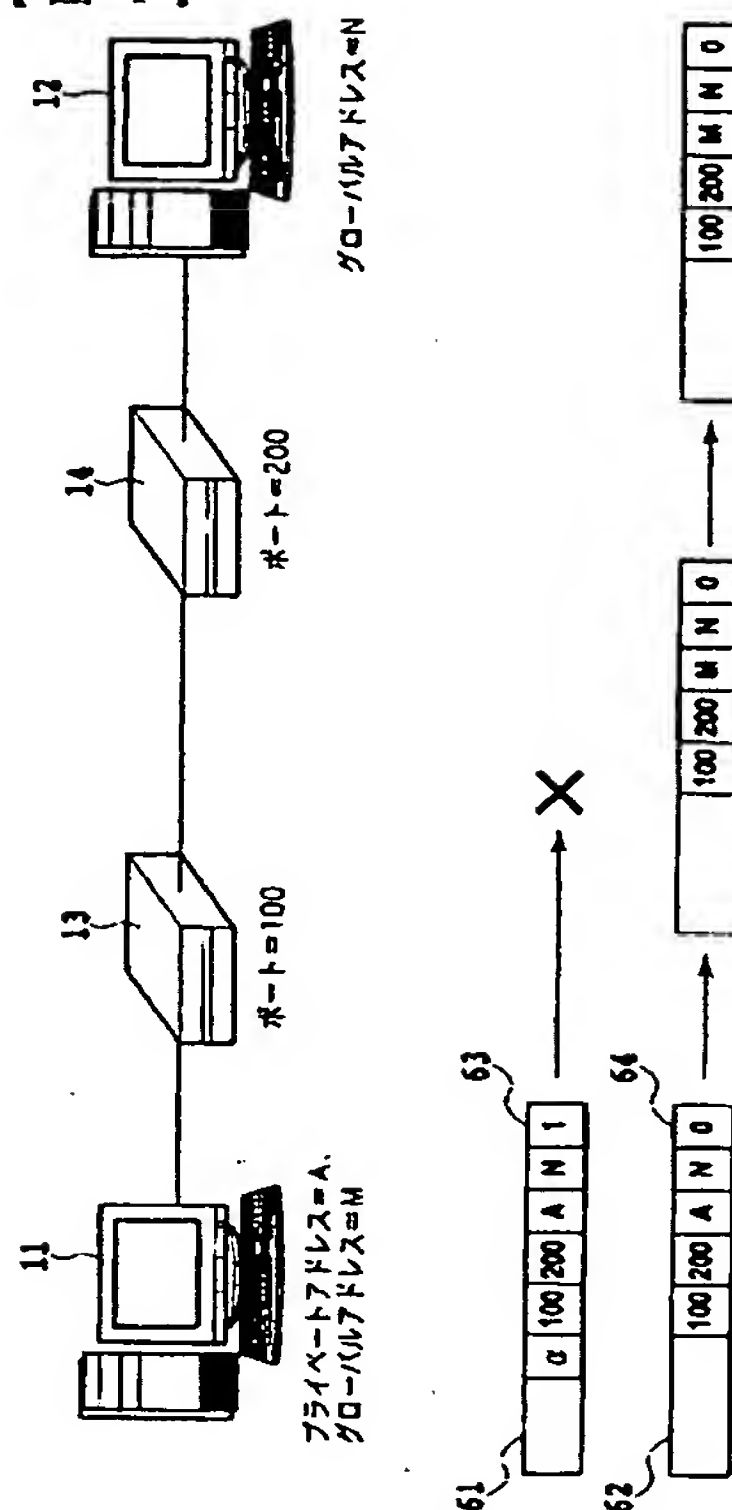
【 図 2 】



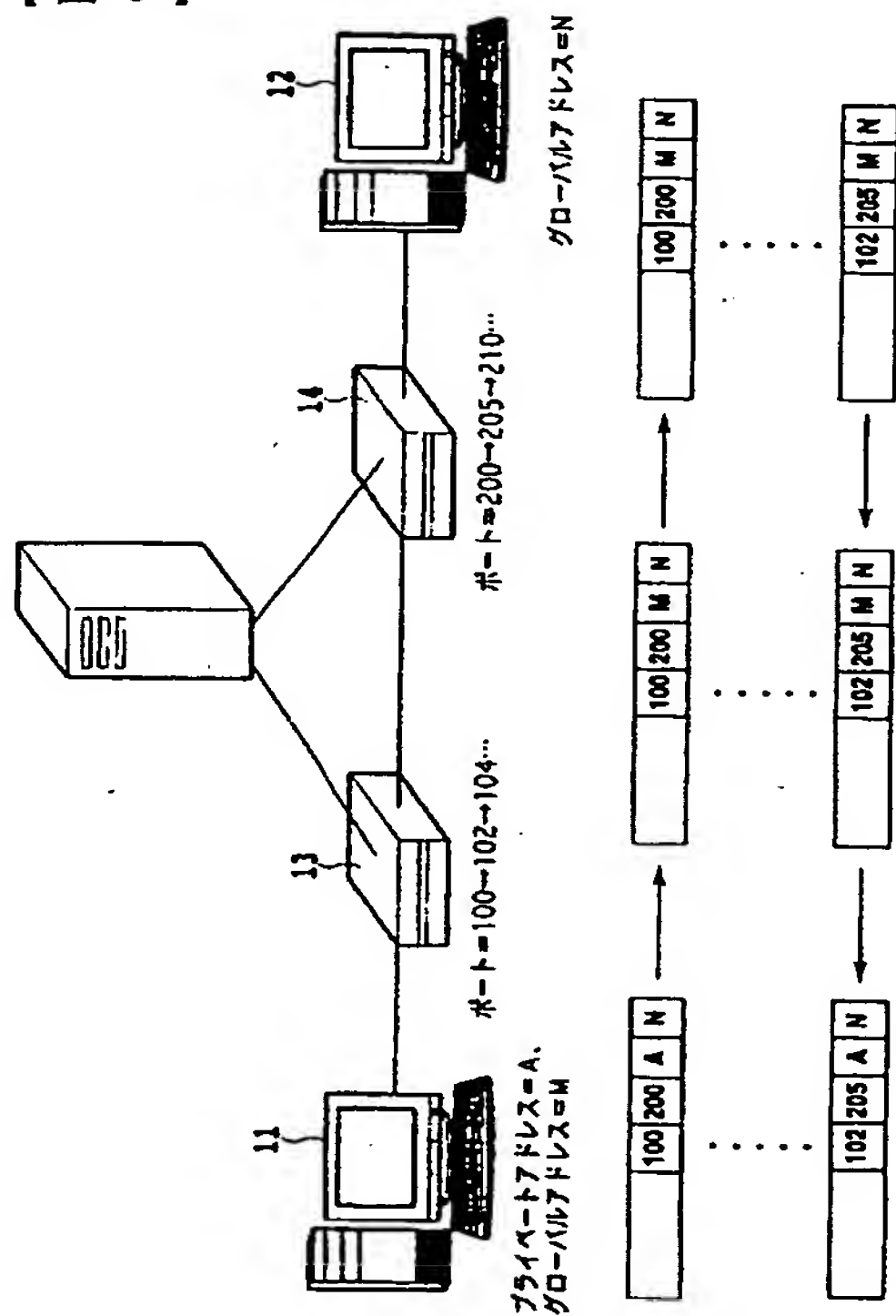
【図 3】



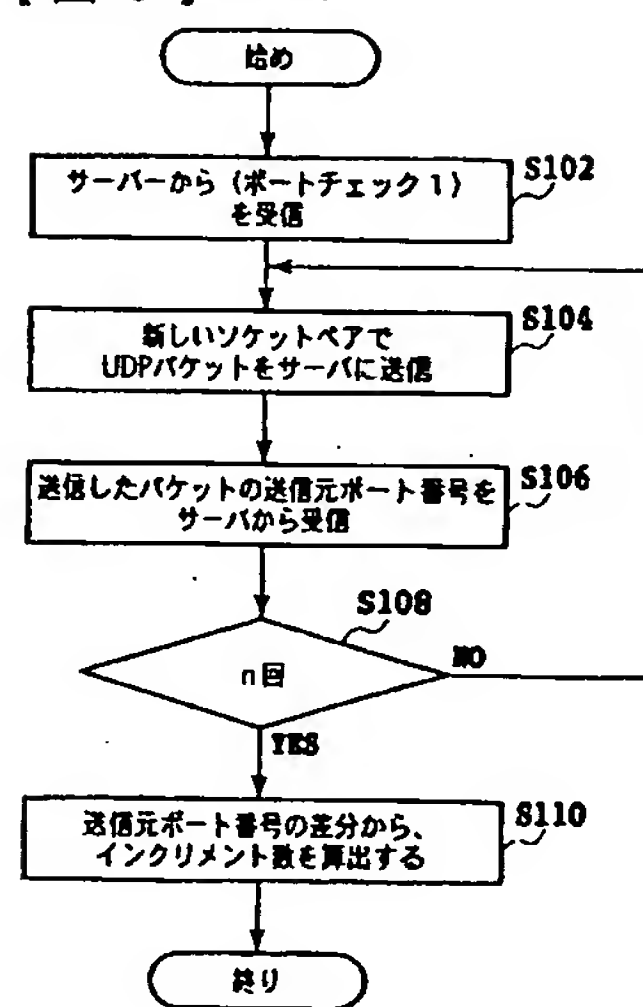
【図 4】



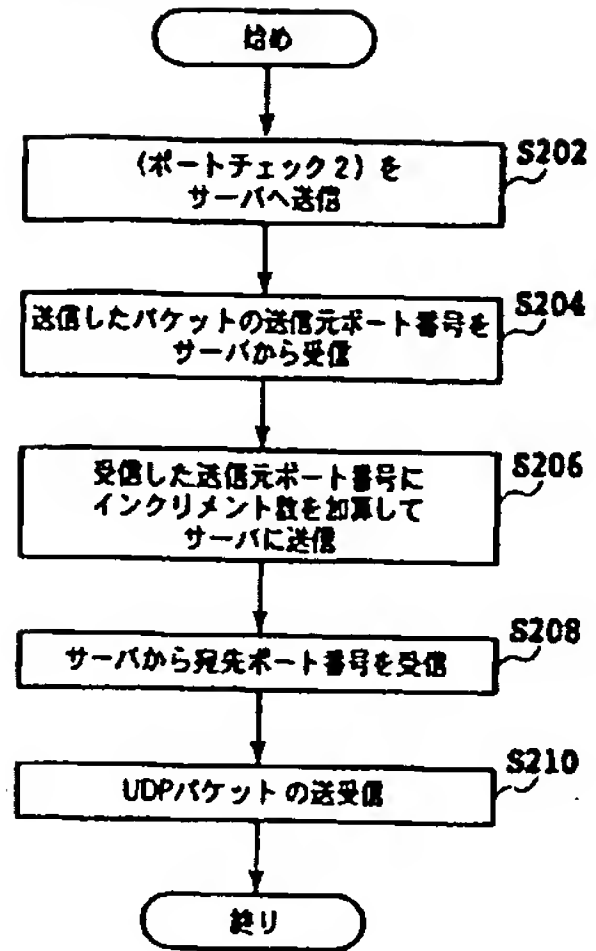
【図 5】



【図 6】



【図 7】



フロントページの続き

(72)発明者 須之内 雄司

神奈川県藤沢市湘南台 1-7-4 株式会社ニューロン内

(72)発明者 荒木 英士

神奈川県藤沢市湘南台 1-7-4 株式会社ニューロン内

(72)発明者 木野瀬 友之

神奈川県藤沢市湘南台 1-7-4 株式会社ニューロン内

Fターム(参考) 5K033 CB01 CB09 DA06

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record.**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☒ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.